Privacy and artificial intelligence: challenges for protecting health information in a new era

Year: 2021 | Citations: 544 | Authors: Blake Murdoch

Abstract

Advances in healthcare artificial intelligence (AI) are occurring rapidly and there is a growing discussion about managing its development. Many AI technologies end up owned and controlled by private entities. The nature of the implementation of AI could mean such corporations, clinics and public bodies will have a greater than typical role in obtaining, utilizing and protecting patient health information. This raises privacy issues relating to implementation and data security. The first set of concerns includes access, use and control of patient data in private hands. Some recent public–private partnerships for implementing AI have resulted in poor protection of privacy. As such, there have been calls for greater systemic oversight of big data health research. Appropriate safeguards must be in place to maintain privacy and patient agency. Private custodians of data can be impacted by competing goals and should be structurally encouraged to ensure data protection and to deter alternative use thereof. Another set of concerns relates to the external risk of privacy breaches through AI-driven methods. The ability to deidentify or anonymize patient health data may be compromised or even nullified in light of new algorithms that have successfully reidentified such data. This could increase the risk to patient data under private custodianship. We are currently in a familiar situation in which regulation and oversight risk falling behind the technologies they govern. Regulation should emphasize patient agency and consent, and should encourage increasingly sophisticated methods of data anonymization and protection.